whalebone

Network Security Threat Landscape

2024 Annual Report

Table of contents

“In the cyber threat landscape, speed is everything. It’s not just about identifying threats but stopping them before they cause damage, and regional intelligence gives us that edge.”

VILIAM PÉLI
WHALEBONE THREAT INTELLIGENCE SPECIALIST

Executive Summary

In 2024, cyber threats became more targeted and sophisticated, with regional attacks and AI-driven techniques taking center stage. More and more, we see attackers tailoring their tactics to local ecosystems, increasing their chances of success. At the same time, evolving techniques like Registered Domain Generation Algorithms (RDGAs), and malicious Cross-site scripting (XSS) made traditional detection even harder.

The ongoing evolution of DNS security played a critical role in fighting these threats. Newly introduced solutions like Microsoft's Zero Trust DNS (ZTDNS) are reshaping how DNS is secured. By adopting principles of zero trust — verifying every connection — organizations can significantly reduce their exposure to evolving threats.

3 Key Learnings from 2024 Cyber Threat Landscape

1. **Phishing campaigns are becoming harder to detect**

   Attackers increasingly use AI to localize phishing websites and messages, making scams more convincing and effective.

2. **Regional threats are on the rise**

   Cybercriminals are tailoring attacks to local ecosystems, exploiting regional vulnerabilities in banks, public services, and political organizations.

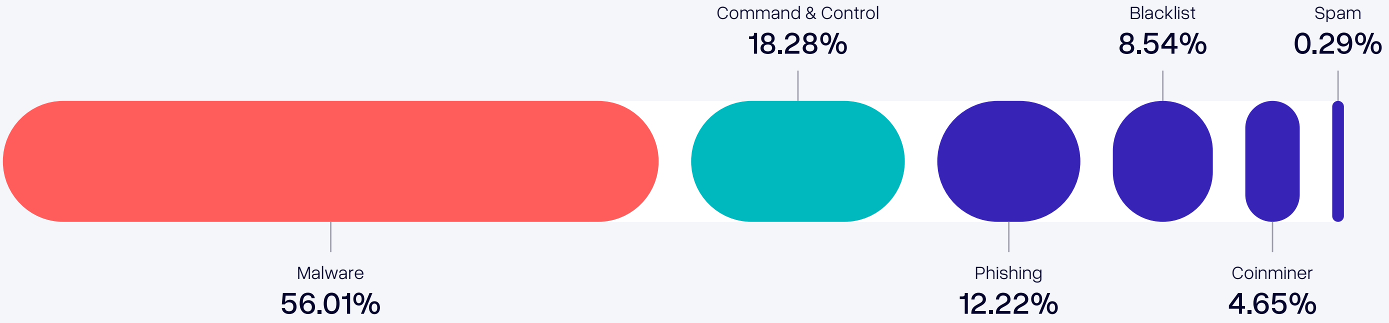
3. **Malware remains the leading threat**

   With constant innovation, malware families like Omnatuor and SpyNote continue to dominate, posing risks to both individuals and businesses worldwide.

Key Learnings

Threats can be categorized based on how they operate. Below is the proportional distribution of threats observed across all malicious traffic analyzed by Whalebone DNS resolvers, regardless of the specific product. This data compares the total number of blocked security incidents involving DNS requests to malicious domains.

The Most Significant Threat Categories



Malware remained the most prevalent threat we mitigated during the analyzed period, with Command & Control coming in second.

Malware continues to be a constant presence across the Internet, affecting users globally throughout the year.

Here Is How the Categories Are Defined

Malware

Domains that host and distribute any kind of malicious code. Malware is a malicious software designed to harm, exploit, or gain unauthorized access to devices, networks, or data.

Command & Control

Domains that facilitate malware (e.g., botnet) communication to coordinate their activities. A botnet is a network of infected devices, which are controlled as a group.

Phishing

Domains that aim to trick users and extract sensitive information such as payment card details, login credentials, etc.

Blacklist

Domains that are known to serve nefarious purposes and are blocked or denied access.

Coinminer

Domains that hijack processing and energy resources for unsolicited cryptocurrency mining.

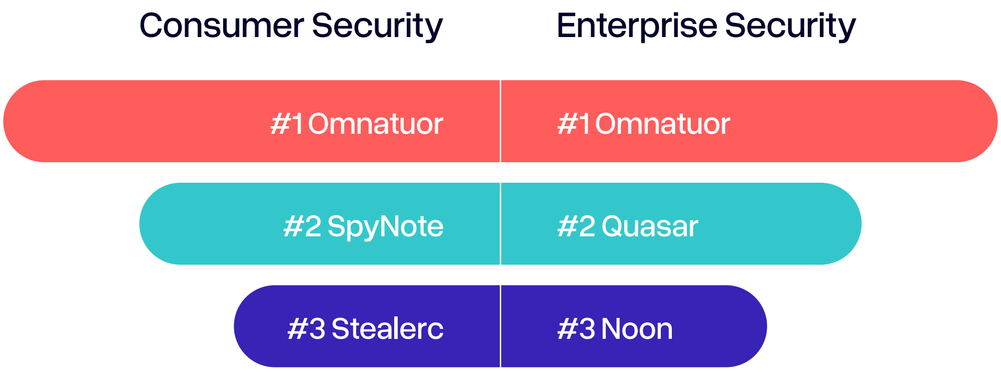
Spam

Domains that are used in spam and scam schemes. This does not only cover emails but also instant messaging and online discussions.

The Most Significant Malware Families

Malware families consist of applications that share similar attack methods and overlapping code. As malware evolves into numerous variants, grouping them into families based on shared traits is crucial for effective threat intelligence.

The graph below highlights the most widespread malware families targeting end users and businesses. These families are ranked by the number of devices attempting to connect to malicious domains associated with them, rather than the total DNS queries. This approach accounts for threats that may generate significant traffic despite limited distribution.



Consumer Security	Enterprise Security
#1 Omnatuor	#1 Omnatuor
#2 SpyNote	#2 Quasar
#3 Stealerc	#3 Noon

What to Expect From These Malware Families?

Omnatuor

Omnatuor is a malicious advertisement network that constantly redirects the browser to other unsafe pages which include ads for dubious browser extensions, fake surveys, compromised online games, adult content, or fake software updates that only install malware. It is a spider's web and once the victim gets caught in it, it is very difficult to escape it.

SpyNote

SpyNote is a type of Android malware that disguises itself as legitimate apps to gain access to devices. It allows attackers to spy on users by stealing sensitive data, recording audio, tracking locations, and even taking full remote control of the infected device.

Stealerc

An information-stealing malware that emerged in early 2023, designed to extract sensitive data from victims' devices, including login credentials, cryptocurrency wallets, and information from applications like Outlook and Telegram. It operates stealthily, often delivered via phishing emails or malicious downloads, and exfiltrates data to remote servers controlled by attackers.

Quasar

A remote access trojan (RAT) primarily targeting Windows systems, designed to give attackers full control over infected devices. It enables activities such as keylogging, data theft, and remote desktop access, often used in cyber-espionage and targeted attacks.

Noon

Trojan, which is usually used as a password stealer or a keylogger (records keystrokes of users).

General Trends

Cyber threats are becoming increasingly regional, with attackers tailoring their methods to exploit local vulnerabilities and target specific industries. These threats are often highly sophisticated, leveraging advanced techniques like localization and regional targeting to bypass traditional global security measures.

This report focuses on the clear shift toward localized cybercrime strategies, requiring constant adaptation to counter evolving tactics. By focusing on regional threat intelligence, we can better predict, detect, and mitigate these threats, ensuring more effective protection for individuals and organizations alike. This approach enables us to address unique challenges and emerging risks in every region we serve.

Threats Pinpointed

Cybersecurity is a fast-moving battlefield, where today's most pressing threats may vanish or evolve by next year. Attackers are always finding new ways to adapt and innovate, which means we need to stay alert and ready to respond to new threats. Every day, new techniques emerge, designed to exploit vulnerabilities, deceive users, and bypass defenses. Here are the three main topics of 2024.

Malvertising

Malvertising, a blend of "malware" and "advertising," involves embedding malicious software within seemingly harmless online ads. These deceptive ads can infiltrate various platforms, from popular websites and social media to mobile apps, posing a significant threat to unsuspecting users.

The effectiveness of malvertising lies in its ability to blend in. Ads are generally perceived as harmless, and a tempting offer can make even the most cautious user click. Additionally, notifications from compromised sites can appear to come from legitimate apps, making it harder to identify the threat.

Phishing

Phishing is a method used by cybercriminals to trick people into sharing sensitive information, such as passwords or financial details, by pretending to be a trusted organization. They often use carefully crafted emails, messages, or websites that mimic legitimate sources, making it difficult to spot the deception at first glance.

In 2024, numerous notable phishing attacks highlighted the evolving tactics of cybercriminals. Unsurprisingly, among the most imitated brands last year were the tech giants Microsoft and Google, followed by fake sites posing as LinkedIn, Apple, DHL, and other global companies.

Additionally, there was a rise in "quishing," where attackers used QR codes to direct victims to malicious sites, exploiting the growing trust and ubiquity of QR technology.

Cross-Site Scripting (XSS)

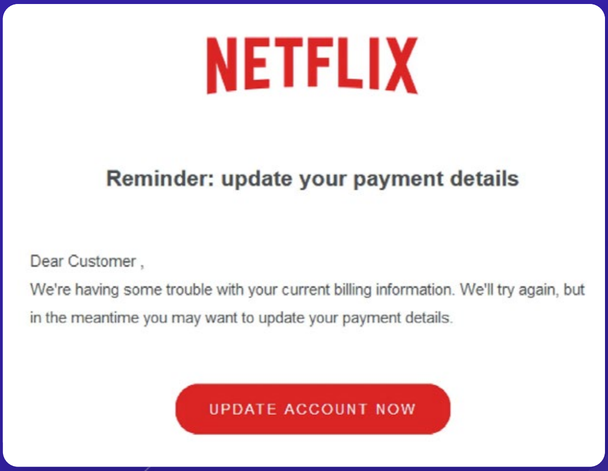
Cross-site scripting (XSS) is a type of security vulnerability where attackers insert malicious code — usually in the form of scripts — into a trusted website or app. When unsuspecting users interact with the compromised page, the malicious code runs in their browser without their knowledge.

This can allow attackers to steal sensitive information like login details, manipulate what users see on the site, or even take control of their accounts. Essentially, XSS tricks your browser into trusting and running harmful code as if it came from a legitimate source.

The Rise of Regional Cyber Threats

Cybersecurity is no longer a global problem alone – it has become deeply regional. One key factor is the **widespread use of AI by cybercriminals to localize and tailor attacks** with unprecedented ease. AI tools enable attackers to quickly translate phishing websites, emails, and scams into native languages, making them **far more convincing and effective in specific regions.** This localization significantly increases the success rate of these campaigns by blending seamlessly into local digital ecosystems.

While standard security measures are effective at blocking generic threats that originate worldwide, they often fall short when it comes to addressing attacks tailored to specific regions. These **locally targeted threats are more sophisticated, harder to trace, and capable of evading traditional defenses.** Only advanced solutions, designed with regional insight, can provide the necessary protection.



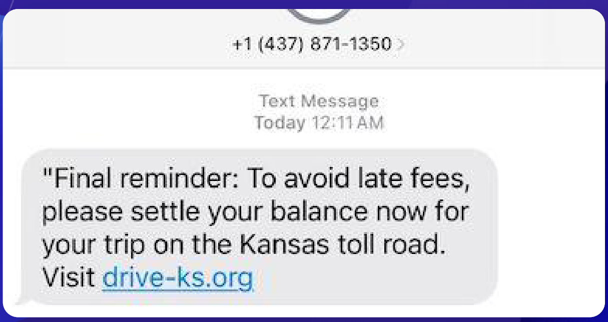
NETFLIX

Reminder: update your payment details

Dear Customer ,
We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

Global phishing email

Standard security blocks common global threats



+1 (437) 871-1350

Text Message
Today 12:11 AM

"Final reminder: To avoid late fees, please settle your balance now for your trip on the Kansas toll road. Visit drive-ks.org

Smishing campaign targeting Kansas

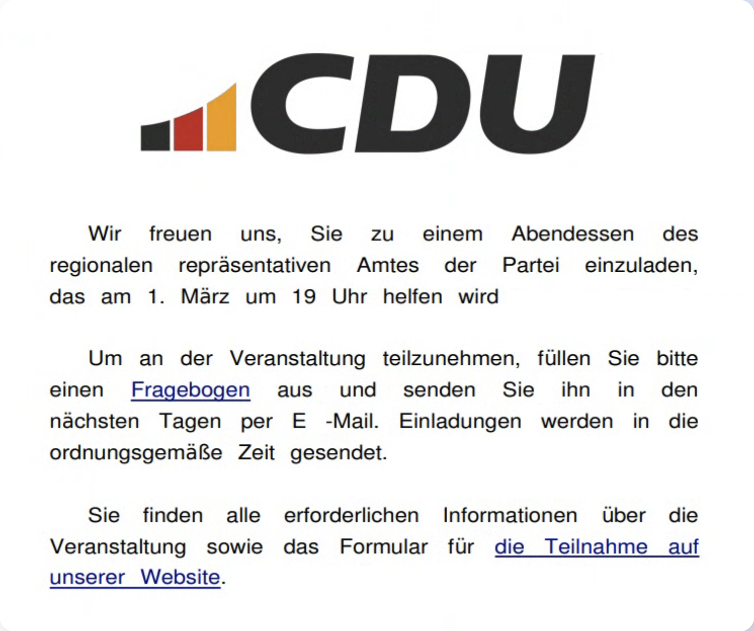
Only the best security blocks also locally targeted threats

> "Global protection is not good enough – you need regional intelligence."

ROBERT SEFR
WHALEBONE CTO

Regional Threats Unveiled

German Political Parties Targeted in Sophisticated Attack



CDU

Wir freuen uns, Sie zu einem Abendessen des regionalen repräsentativen Amtes der Partei einzuladen, das am 1. März um 19 Uhr helfen wird

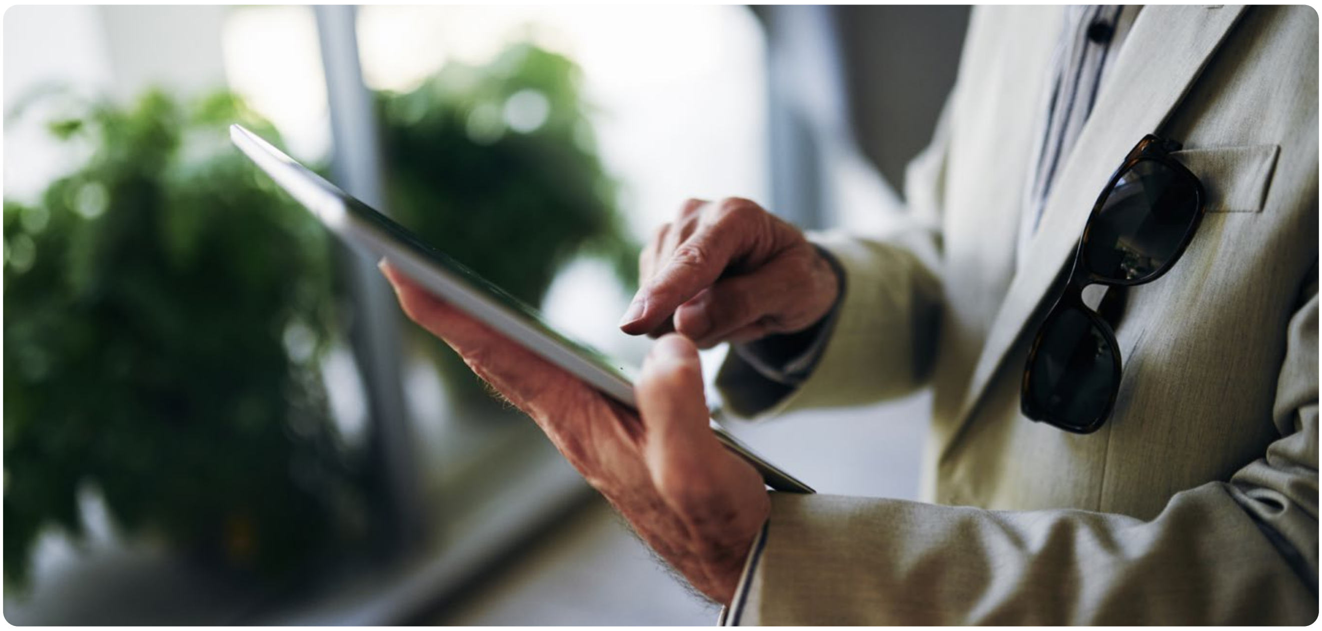
Um an der Veranstaltung teilzunehmen, füllen Sie bitte einen Fragebogen aus und senden Sie ihn in den nächsten Tagen per E -Mail. Einladungen werden in die ordnungsgemäße Zeit gesendet.

Sie finden alle erforderlichen Informationen über die Veranstaltung sowie das Formular für die Teilnahme auf unserer Website.

APT29, a hacking group linked to Russia's Foreign Intelligence Service and active since at least 2008, recently launched a deceptive campaign targeting unsuspecting users through compromised WordPress sites.

These sites were ingeniously crafted to appear as legitimate invitations to a fake event purportedly hosted by Germany's Christian Democratic Union (CDU). Victims who clicked on the links were redirected to a malware installer known as ROOTSAW, designed to infiltrate their systems.

Thanks to our proactive detection measures, we blocked **37 attempts** to access these malicious sites, effectively neutralizing the threat before the compromised content was removed.



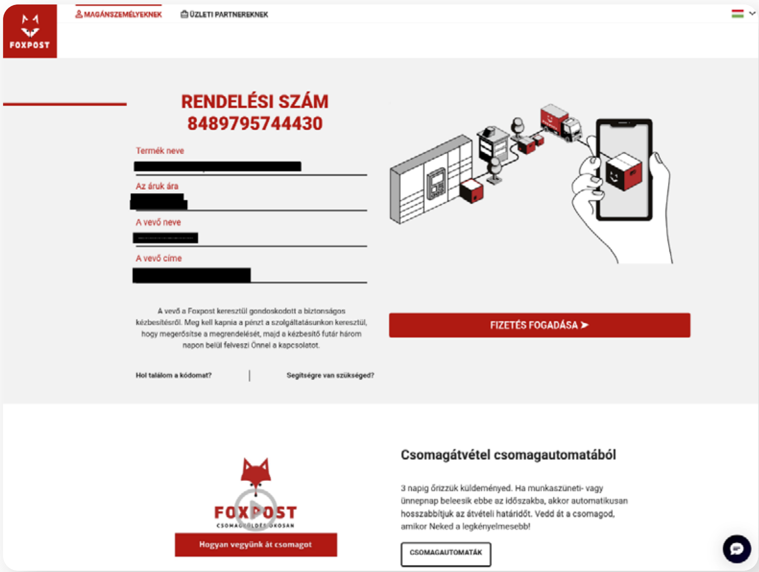
Marketplace Phishing Targeting Hungary’s Banks

A new wave of Marketplace phishing attacks has targeted Hungary’s banks, posing as online marketplaces, delivery services, or shops to deceive victims. These scams redirect users to fake banking screens designed to steal sensitive login details. Attackers relied on a single domain, altering subdomains to evade detection and launch multiple attack vectors, showcasing constant innovation and adaptability.

Whalebone has blocked over **200 unique domains**, disrupting these campaigns before they could harm users. We are closely monitoring and blocking both direct attacks and those originating from the bazaars wherever possible.

Phishing Domain

https://foxpost.clientorder-online.com/order/merchant/1ZblbQWq/



RENDELÉSI SZÁM 8489795744430

Termék neve
[redacted]

Az áruk ára
[redacted]

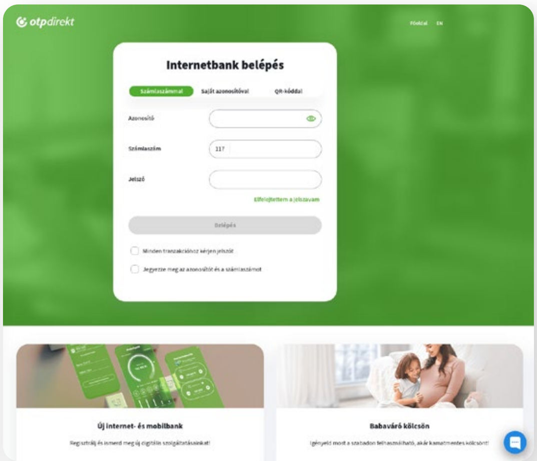
A vevő neve
[redacted]

A vevő címe
[redacted]

A vevő a Foxpost keresztül gondoskodott a biztonságos kézbesítésről. Meg kell kapnia a pénzt a szolgáltatásunkon keresztül, hogy megerősítse a megrendelését, majd a kézbesítő futár három napon belül felveszi Önnel a kapcsolatot.

Csomagátvétel csomagautomatából

3 napig őrizzük küldeményed. Ha munkaszüneti- vagy ünnepnap beleesik ebbe az időszakba, akkor automatikusan hosszabbítjuk az átvételi határidőt. Vedd át a csomagod, amikor Neked a legkényelmesebb!



Internetbank belépés

Azonosító

Számlaszám 117

Jelszó

□ Minden tranzakcióhoz kérjen jelszót

□ Jegyezze meg az azonosítót és a számlaszámot

Új internet- és mobilbank

Regisztrálj és ismerd meg új digitális szolgáltatásainkat!

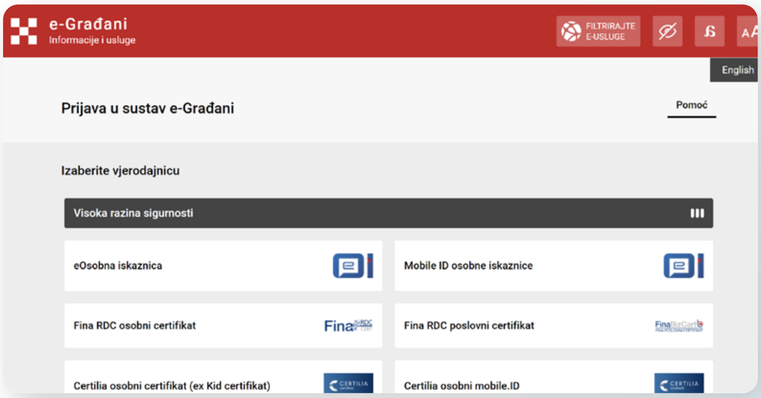
Babaváró kölcsön

Igényeld most a szabadon felhasználható, akár kamatmentes kölcsönt!

Spoofed Governmental Services in Croatia

Malicious domains exploiting the term “prijava” (login/registration) have increasingly targeted governmental services in Croatia, posing a significant threat to users. Domains like *****-prijava-hr[.]com* and *prijava-****[.]firebaseapp.com* mimic legitimate services to deceive users and steal sensitive information.

These threats are not confined to Croatia — they also target other countries in the former Yugoslavian region. By continuously refining our regional threat intelligence, we can better detect and block these attacks, ensuring more people are protected from these deceptive schemes.

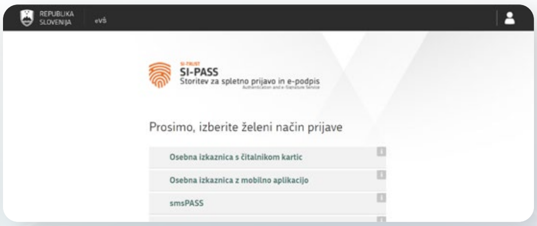


Prijava u sustav e-Građani

Izaberite vjerodajnicu

Visoka razina sigurnosti

eOsobna iskaznica	Mobile ID osobne iskaznice
Fina RDC osobni certifikat	Fina RDC poslovni certifikat
Certilia osobni certifikat (ex Kid certifikat)	Certilia osobni mobile.ID



Prosimo, izberite želeni način prijave

- Osebna izkaznica s čitalnikom kartic
- Osebna izkaznica z mobilno aplikacijo
- smsPASS

Whalebone Solution

Regional Threat Intelligence Research & CERT Information Exchange

To counter these emerging threats, our approach integrates **Regional Threat Intelligence and close partnerships with local CERTs** (Computer Emergency Response Teams). By combining our research with the local expertise of CERTs and utilizing platforms like MISP (Malware Information Sharing Platform), we share actionable intelligence swiftly across Europe.

This collaboration ensures **faster detection of threats**, including regionally focused attack patterns like the movement of malware campaigns between countries. Our solution continuously adapts, and proactively blocks these evolving threats before they reach end-users.

Our real-time detection capabilities take this protection even further. **By spotting and stopping AI-generated attacks, we neutralize these threats as soon as they appear**. This agility, coupled with our expertise in covering local threats like phishing, smishing, and malware, ensures we can adapt to evolving risks faster than attackers can exploit them.

Whether it is blocking harmful websites or tailoring optional content filters to local needs (like gambling or gaming restrictions), Whalebone delivers **precise, proactive security** tailored to the unique challenges of each local environment.

Learn more in our Threat Intelligence White Paper

Sign Up →

Would you like to discuss our Threat Intelligence with an expert?
Feel free to contact our Threat Intelligence Lead
Follow us
www.whalebone.io
whalebone
Whalebone Threat Intelligence
Real Difference, Real-Time

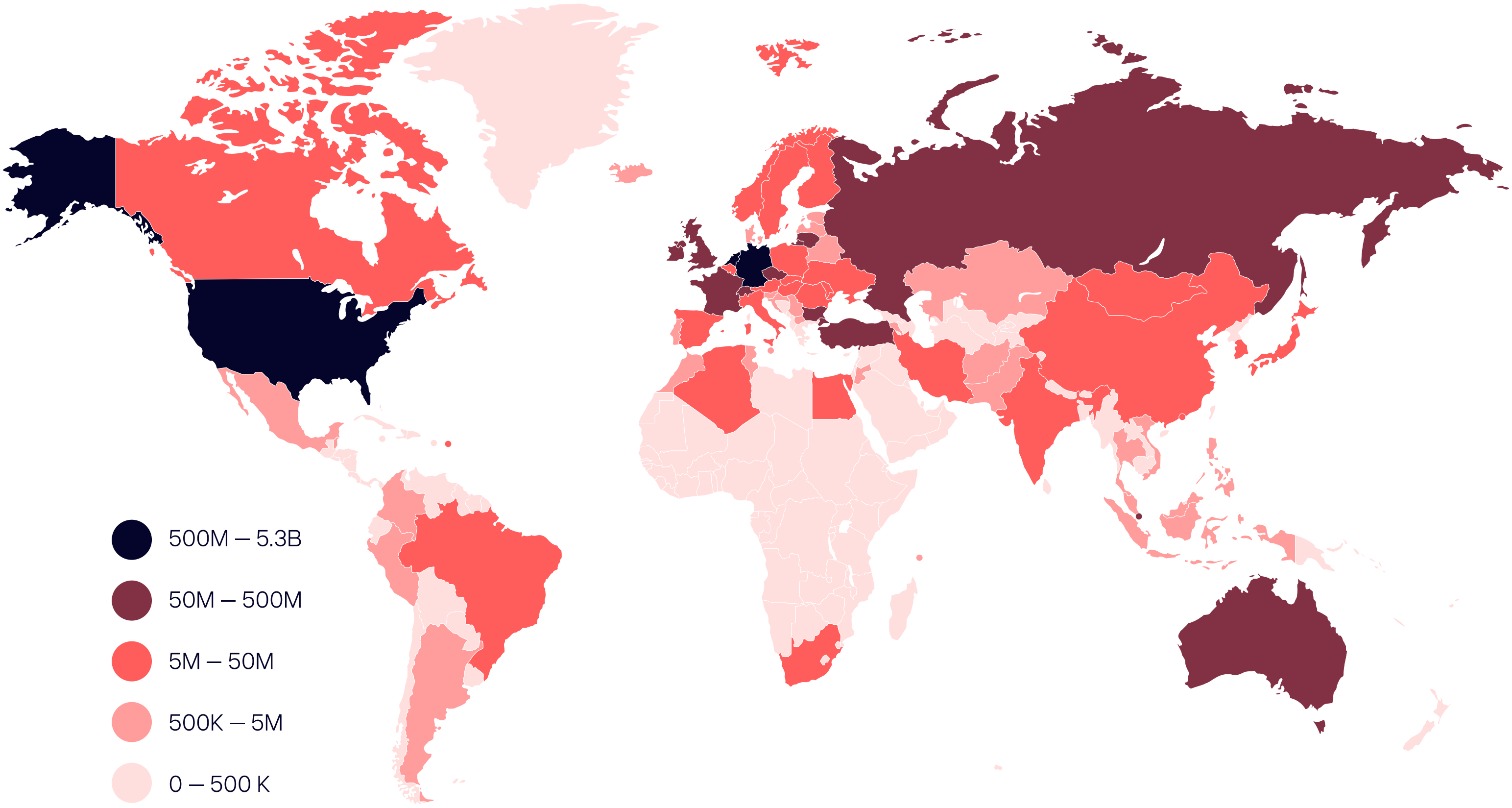
Threat Landscape in 2024

In 2024, we witnessed an increasing variety of cyber threats, with a notable rise in their overall volume. While the landscape of online threats continues to evolve, some patterns remain consistent. This chapter explores some of the most noteworthy threats observed over the past year.

Geographical Distribution of Cyber Threats

Cyber threats come from all corners of the Earth. The map highlights regions where Whalebone products successfully thwarted threats, showcasing the geographical distribution of these attacks.

It is important to note that the highlighted countries, which host some of the world's largest cloud and hosting infrastructures widely used across the globe, are not necessarily the source of the cyber threats displayed.



Phishing: The Art of Deception

Phishing continues to be a favored method for spreading malware and stealing sensitive information like payment card details and passwords. Attackers typically use emails, text messages, or app notifications to pressure users into taking immediate action.

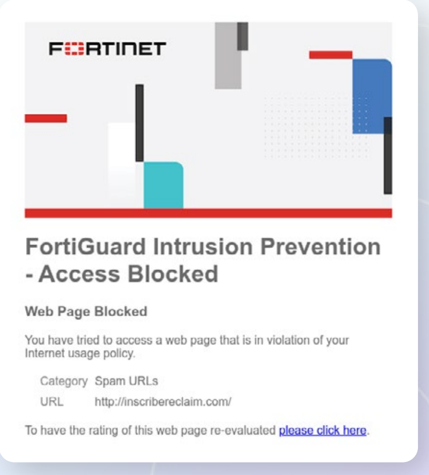
To deceive even cautious users, cybercriminals create realistic fake websites, use interchangeable domain names, and tailor messages to specific audiences, often translating content into the target language for added authenticity.

Fortunately, Whalebone DNS resolvers are highly effective at detecting irregularities and blocking phishing attempts. By utilizing threat intelligence feeds and honeypots, Whalebone identifies phishing links before users can access them. With our global reach, we track the latest phishing campaigns. Here are some notable examples from 2024.

Fake Antivirus, Real Threat

Throughout 2024, users in certain regions encountered fake antivirus pop-ups designed to look like legitimate warnings. These pop-ups claimed to have blocked access to a malicious website but were themselves part of a phishing scam. Their goal? To trick users into revealing personal information or handing over money.

The irony of hackers impersonating antivirus tools is a stark reminder to stay cautious. Always verify that security alerts come from your actual antivirus software, not from random websites or pop-ups encountered while browsing.



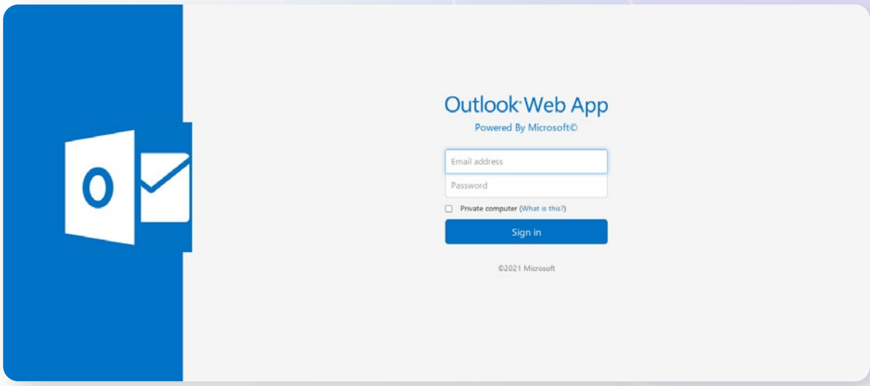
FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

You have tried to access a web page that is in violation of your Internet usage policy.

Category Spam URLs
URL http://inscribereclaim.com/

To have the rating of this web page re-evaluated please click here.



Outlook Web App
Powered By Microsoft©

□ Private computer (What is this?)

©2021 Microsoft

Outlook Fraud to Trap Your Credentials

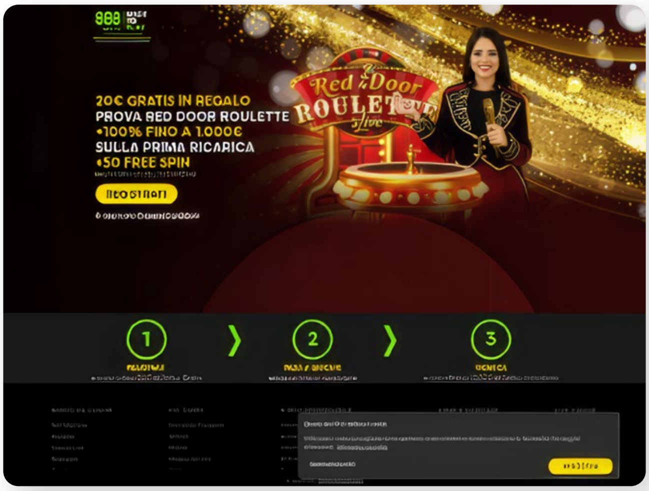
Users across the globe were tricked by a phishing scam pretending to be the popular email platform Outlook. The fake site looked almost identical to the real login page, making it easy for people to enter their email and password without suspecting anything. These malicious links were often sent via email or SMS, claiming that users needed to "verify their account for protection." Ironically, this led to their accounts being breached.

The scam works by using links that look like the real thing but may have small differences, like a single letter changed or characters written in Punycode. Once attackers gain access, they use the victim's email to target their contacts, spreading the scam further. Fake login pages like this remain one of the most common and effective phishing tactics globally. Always double-check links before logging in to protect your accounts.

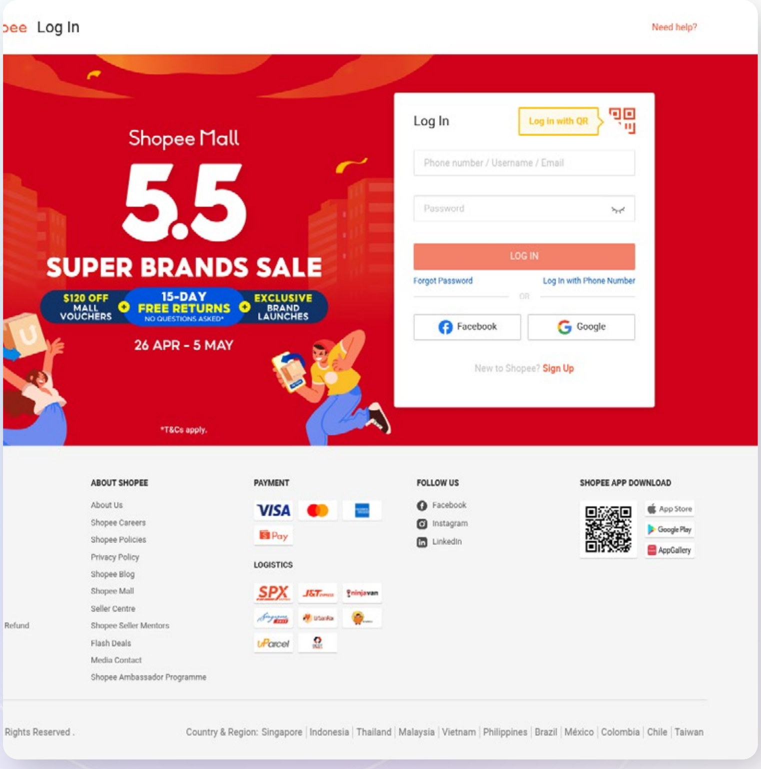
Rigged from the Start: Fake Casinos Preying on Players

One of the more sophisticated scams users may have encountered throughout the past year was a fake online casino. Unlike typical gambling pop-up scams, this site appeared almost legitimate and harmless at first glance. However, a closer look revealed several red flags.

The site was newly created, with little to no social media presence — a suspicious sign for an online casino. These details strongly suggest it was just another phishing trap designed to steal personal information and financial assets from unsuspecting users.



Hooked by False Deals



A phishing scam disguised as a well-known online store Shopee Mall has been targeting users in Asia through deceptive emails promising exclusive sales and special prices. The site mimics a legitimate e-commerce platform to appear credible, tricking users into sharing sensitive information.

Once on the site, victims are prompted to enter their email addresses, passwords, and, in some cases, even banking credentials under the pretense of payment processing. This scam aims to steal personal and financial data. Fake e-shops like are the evergreen of global threat landscape, which only emphasizes the need to verify online stores before sharing any information with them.

Coinmining Is Back in the Game

With the skyrocketing popularity of cryptocurrency investments, especially Bitcoin, both the legitimate miners and the sneaky hackers are back in action.

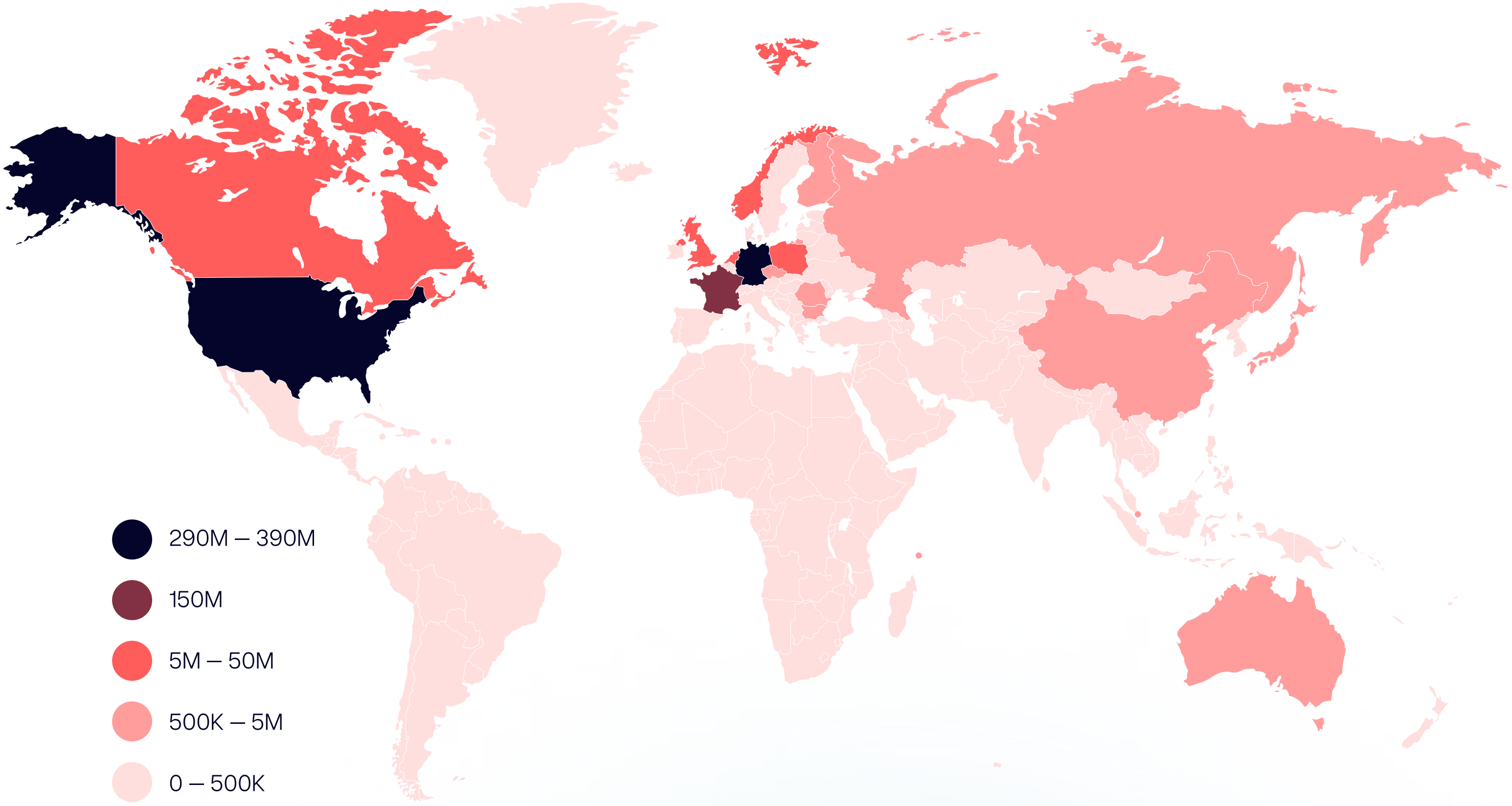
In the past, the earnings from mining typically fell short of covering even the most essential utility bills. Yet, in 2024, it became more and more profitable in most regions across the globe.

Domains Related to Crypto

Whalebone identifies cryptocurrency mining attacks and is able to spot the trends in the threat landscape. Throughout all of our customers' network activities, we stopped over **1.4 billion crypto mining pool–related requests**. Throughout the past year, we have seen a steady increase in mining activity.

The most popular mined cryptocurrency remains **Monero (XMR)** as it is the most widely spread cryptocurrency which is truly anonymous.

The following map shows the proportional geographical distribution of crypto pools



Command & Control

Command and Control (C&C or C2) refers to how cybercriminals communicate with and control devices they have infected with malware. Once a device is compromised, it becomes part of their network, often called a botnet. The C&C server acts like the "brain" of this operation, sending instructions to the infected devices and receiving stolen data or updates from them.

For example, the C&C server might tell infected devices to send out spam emails, steal passwords, or launch attacks on other systems. It acts as a remote control that the attackers use to manage their malicious activities. Without the C&C, the attackers would lose control of the infected devices.

The challenge for hackers is that relying on a single server or access point makes it easy for security solutions to block them. To overcome this, they use Domain Generation Algorithms, which constantly create new domains to avoid detection and maintain their operations.

Domain Generation Algorithm (DGA)

DGAs create numerous domain names that malware uses to communicate with command and control servers, making it difficult for security measures to block malicious traffic effectively.

Recent developments include the emergence of Registered Domain Generation Algorithms (RDGAs), which are more challenging to detect and defend against as the previously algorithmically generated domain names are turned into active, functional, "legitimate" domains that can be used for malicious purposes.

These RDGAs are employed not only for malware distribution but also for phishing, spam, and other malicious activities.

Unmasking Malicious DNS Tunnels

What Are DNS Tunnels?

DNS, the Internet's "phonebook," translates website names into IP addresses, making it essential for online connectivity. However, its near-universal access makes it a prime target for hackers, who exploit it through DNS tunnels — covert channels that send encoded data disguised as legitimate DNS requests.

Why Are They Dangerous?

Malicious DNS tunnels enable hackers to steal data, gain remote access, or maintain command and control over compromised systems. While they operate at low speeds, their stealthy nature can make detection challenging. Abnormal traffic patterns or sudden spikes in DNS requests often signal their presence.

Balancing Security and Functionality

Not all DNS tunnels are harmful — many support essential services like antivirus updates. Effective solutions (like Whalebone) analyze traffic patterns to block malicious tunnels while allowing legitimate ones. By leveraging advanced algorithms and monitoring tools, these defenses ensure security without disrupting vital Internet functionality.

The Evolution of DNS Security: From DoH to ZTDNS

For decades, the DNS protocol — the “phonebook of the internet” — has operated without privacy or security at its core. However, with growing cybersecurity threats, this vital system has evolved. Privacy-focused advancements like [DNS over HTTPS (DoH) and DNS over TLS (DoT)]() brought encryption to DNS queries, making them more secure from interception.

Now, [Microsoft’s Zero Trust DNS]() **(ZTDNS)** represents the next step, embedding the principles of zero trust — “never trust, always verify” — into DNS security.

ZTDNS improves security by allowing only connections that have been verified through trusted DNS queries. This helps block unauthorized access, prevent data breaches, and stop attackers from controlling compromised devices. By requiring strict identity checks and carefully monitoring DNS traffic, ZTDNS fixes weaknesses in traditional DNS and supports broader zero-trust security strategies. It shows how vital DNS has become in protecting modern digital systems.

Learn more about ZTDNS →

5 Steps to Success

Our free, 5-step Product Manager Guide email series is designed to help telco PMs looking to gain a competitive edge and successfully sell security VAS.

With our Product Manager Guide, you can empower your team to deliver security solutions that your customers will adopt and trust.

Together, these chapters will help you build a compelling case for Whalebone’s security solution, ensuring you have the tools to make our white-label telco security product a success in your portfolio.

Get our Product Manager Guide →

DNS4EU

Enhancing Cybersecurity for EU Citizens

The DNS4EU project, initiated by the European Commission, aims to establish a robust alternative to existing public DNS resolvers, prioritizing security and privacy compliance for up to 100 million EU citizens, companies, and institutions. Whalebone was chosen to lead the consortium of 13 members from 10 countries, tasked with the development and operation of the official DNS resolver for the European Union.

> “Our work with the Consortium, Associated Partners, CERTS, CSIRTs, and other national cybersecurity agencies aims to reduce the likelihood of catastrophic attacks on critical European infrastructure. The idea is that a malicious threat discovered in one country can be blocked more quickly to prevent spreading across multiple regions.”

MAGDALENA KRUCKA
MARKETING MANAGER
FOR DNS4EU

Solutions are readily available for DNS4EU, with DNS4GOV available for organizations outside the EU. Many new initiatives are already underway in the areas of:

- **Onboarding and collaboration** – This collaborative effort aims to extend protective services to the entire government and public infrastructure.
- **Threat Intelligence sharing** – The Consortium is in contact with almost 40 CERTs across Europe – for both public and private sectors.
- **Engagement and outreach** – Whalebone has actively participated in conferences, workshops, and webinars, growing the DNS4EU stakeholder community to over 500 members, reflecting the widespread interest and support for the initiative.

Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) have proven crucial to DNS4EU, providing significant threat intelligence to help improve threat detection and real-time awareness.

National Centers for Cybersecurity (NCSCs) guide government institutions and the public on cybersecurity, often providing DNS4EU services (or DNS4GOV outside the EU) with infrastructure from Whalebone.

Telcos partnered with DNS4EU are able to leverage their infrastructures and government connections for nationwide deployment of the protective DNS service.

Join the initiative →

Conclusion

The 2024 threat landscape shows that cybercriminals are adapting faster than ever, blending technical innovation with targeted strategies to exploit vulnerabilities. Malware and phishing remain dominant, but the resurgence of coinmining and the emergence of RDGAs demonstrate how attackers continue to refine their methods.

At Whalebone, we have seen firsthand how collaboration, regional intelligence, and cutting-edge DNS security make all the difference. By focusing on real-time detection and building tailored defenses, we are ready to protect individuals, businesses, and institutions from evolving threats. Staying ahead in cybersecurity requires vigilance, adaptability, and constant collaboration – **because the threats will always evolve, and so must we**.

Whalebone Products

Aura

Telco Cybersecurity

→

Immunity

Enterprise Cybersecurity

→

Peacemaker

ISP Cybersecurity

→

Whalebone, s.r.o.
Company ID: 05120403
VAT No.: CZ05120403

Jezuitská 14/13
602 00 Brno
Czech Republic

Contributors
Anna Pavlík Rybníčková
Magdalena Krucká

Threat Intelligence Support
Jiří Bordovský
Viliam Péli

Graphic Design
Adam Marcilis

sales@whalebone.io

www.whalebone.io

Follow us